CLAIMS

What is claimed is:

1. A method for initialization of secure communication between a network resource and a client via a network, comprising:

receiving an access at a network resource from a management application of a client;

in response to the access, generating configuration parameters for initializing secure communication with the client via the network;

printing security configuration information showing the configuration parameters, the security configuration information for enabling manual input of the configuration parameters into the management application; and

implementing secure communication with the management application in accordance with the configuration parameters.

2. The method of claim 1 wherein the network resource is a print server and the security configuration information is printed using a printer coupled to the print server.

3. The method of claim 1 wherein the secure communication is in accordance with a version of SNMPv3 standards.

4. The method of claim 1 further comprising:

generating random security parameters to generate the configuration parameters for initializing the secure communication with the client.

5. The method of claim 1 further comprising:

setting a security configuration print page object in response to receiving the access from the management application.

6. The method of claim 5 wherein the security configuration print page object is in accordance with a version of SNMPv3 standards.

7. A network resource system for initializing secure communication with a client via a network, comprising:

a printer; and

a network device coupled to the printer, the network device coupled to the network for communication with a client, the network device having a computer system including a memory storing computer readable code which when executed by the computer system cause the network device to implement a method comprising:

generating configuration parameters for initializing secure communication with the client via the network in response to an access request from the client;

issuing a print command to the printer to print a security configuration page showing the configuration parameters, the security configuration page for enabling manual input of the configuration parameters into a management application of the client; and

implementing secure communication with the management application in accordance with the configuration parameters.

8. The system of claim 7 wherein the secure communication is in accordance with a version of SNMPv3 standards.

9. The system of claim 7 further comprising:

generating random security parameters to generate the configuration parameters for initializing the secure communication with the client.

10. The system of claim 7 further comprising:

setting a security configuration print page object in response to receiving the access from the client.

11. The system of claim 10 wherein the security configuration print page object is in accordance with a version of SNMPv3 standards.

12. The system of claim 7 wherein the network device is a print server.

13. A system for initialization of secure communication between a network resource and a client via a network, comprising:

means for receiving an access at a network resource from a management application of a client;

means for generating configuration parameters for initializing secure communication with the client via the network, in response to the access;

means for printing a security configuration page showing the configuration parameters, the security configuration page for enabling manual input of the configuration parameters into the management application; and

means for implementing secure communication with the management application in accordance with the configuration parameters.

14. The system of claim 13 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

15. The system of claim 13 wherein the means for implementing secure communication are in accordance with a version of SNMPv3 standards.

16. The system of claim 13 further comprising:

means for generating random security parameters to generate the configuration parameters for initializing the secure communication with the client.

17. The system of claim 13 further comprising:

means for setting a security configuration print page object in response to receiving the access from the management application.

18. The system of claim 17 wherein the means for setting a security configuration print page object are in accordance with a version of SNMPv3 standards.

19. A network resource system for initializing secure communication with a client via a network, comprising:

a network interface for receiving an access via a network from a management application of a client;

an SNMP daemon configured to generate configuration parameters for initializing secure communication with the client via the network, in response to the access;

the SNMP daemon configured to generate a configuration page event causing a printer coupled to the network resource to print a

security configuration page showing the configuration parameters, the security configuration page for enabling manual input of the configuration parameters into the management application to implement secure communication.

20. The system of claim 19 further comprising:

an SNMP user table within a data structure of the network resource, the SNMP user table for access by the SNMP daemon and configured to store a user account created in accordance with the configuration parameters.

21. The system of claim 19 wherein the network resource is a print server.

22. The system of claim 19 wherein the SNMP daemon is configured to implement secure communication in accordance with a version of SNMPv3 standards.

23. The system of claim 19 wherein the SNMP daemon is configured to generate random security parameters in order to generate the configuration parameters for initializing the secure communication.

24. The system of claim 19 wherein the network interface includes a plurality of interface components for interfacing with a corresponding plurality of network communication protocols.

25. The system of claim 24 wherein the network communication protocols include TCP/IP, IPX, and Apple Talk

26. A method for initialization of secure communication between a network resource and a client via a network wireless access point, comprising:

receiving an ad hoc access at a network resource from a management application of a client;

in response to the ad hoc access, generating a security key for initializing secure communication with the client via a wireless access point;

printing a security configuration page showing the security key, the security configuration page for enabling manual input of the security key into the management application;

receiving an encrypted ad hoc access in accordance with the security key from the management application to configure infrastructure mode parameters for the wireless access point; and

implementing secure communication with the management application in accordance with the security key via the wireless access point in infrastructure mode.

27. The method of claim 26 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

28. The method of claim 26 wherein the secure communication is in accordance with a version of 802.11 standards.

29. The method of claim 26 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication with the client.

30. The method of claim 26 further comprising:

setting a 802.11 security configuration print page object in response to receiving the ad hoc access from the management application.

31. A system for initialization of secure communication between a network resource and a client via a network wireless access point, comprising:

a printer; and

a network device coupled to the printer, the network device coupled to the network for communication with a client, the network device having a computer system including a memory storing computer readable code which when executed by the computer system cause the network device to implement a method comprising:

generating a security key for initializing secure communication with the client via the wireless access point in response an ad hoc access from a management application of a client;

issuing a print command to the printer to print a security configuration page showing the security key, the security configuration page for enabling manual input of the security key into the management application;

receiving an encrypted ad hoc access in accordance with the security key from the management application to configure infrastructure mode parameters for the wireless access point; and

implementing secure communication with the management application in accordance with the security key via a wireless access point in infrastructure mode.

32. The system of claim 31 wherein the network device is a print server.

33. The system of claim 31 wherein the secure communication is in accordance with a version of 802.11 standards.

34. The system of claim 31 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication with the client.

35. The system of claim 31 wherein the method implemented by the network device further comprises:

setting a 802.11 security configuration print page object in response to receiving the ad hoc access from the management application.

36. A system for initialization of secure communication between a network resource and a client via a network wireless access point, comprising:

means for receiving an ad hoc access at a network resource from a management application of a client;

means for generating a security key for initializing secure communication with the client via a wireless access point in response to the ad hoc access;

means for printing a security configuration page showing the security key, the security configuration page for enabling manual input of the security key into the management application;

means for receiving an encrypted ad hoc access in accordance with the security key from the management application to

configure infrastructure mode parameters for the wireless access point; and

means for implementing secure communication with the management application in accordance with the security key via the wireless access point in infrastructure mode.

37. The system of claim 36 wherein the network resource is a print server and the means for printing a security configuration page comprises a printer coupled to the print server.

38. The system of claim 36 wherein the means for implementing secure communication is in accordance with a version of 802.11 standards.

39. The system of claim 36 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication means with the client.

40. The system of claim 36 further comprising:

setting a 802.11 security configuration print page object in response to receiving the ad hoc access from the management application.

41. A computer readable media having computer readable code which when executed by a computer system of a network resource causes the network resource to implement a method for initialization of secure communication between the network resource and a client via a network, comprising:

receiving an access at a network resource from a management application of a client;

in response to the access, generating configuration parameters for initializing secure communication with the client via the network;

printing a security configuration page showing the configuration parameters, the security configuration page for enabling manual input of the configuration parameters into the management application; and

implementing secure communication with the management application in accordance with the configuration parameters.

42. The computer readable media of claim 41 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

43. The computer readable media of claim 41 wherein the secure communication is in accordance with a version of SNMPv3 standards.

44. The computer readable media of claim 41 further comprising:

generating random security parameters to generate the configuration parameters for initializing the secure communication with the client.

45. The computer readable media of claim 41 further comprising:

setting a security configuration print page object in response to receiving the access from the management application.

46. The computer readable media of claim 45 wherein the security configuration print page object is in accordance with a version of SNMPv3 standards.

47. A computer readable media having computer readable code which when executed by a computer system of a network resource causes the network resource to implement a method for initialization of secure communication between the network resource and a client via a network wireless access point, comprising:

receiving an ad hoc access at a network resource from a management application of a client;

in response to the ad hoc access, generating a security key for initializing secure communication with the client via a wireless access point;

printing a security configuration page showing the security key, the security configuration page for enabling manual input of the security key into the management application;

receiving an encrypted ad hoc access in accordance with the security key from the management application to configure infrastructure mode parameters for the wireless access point; and

implementing secure communication with the management application in accordance with the security key via the wireless access point in infrastructure mode.

48. The method of claim 47 wherein the network resource is a print server and the security configuration page is printed using a printer coupled to the print server.

49. The method of claim 47 wherein the secure communication is in accordance with a version of 802.11 standards.

50. The method of claim 47 wherein the security key is a randomly generated 802.11 Wired Equivalent Privacy key for initializing the secure communication with the client.

51. The method of claim 47 further comprising:

setting a 802.11 security configuration print page object in response to receiving the ad hoc access from the management application.